Brief Introduction to Linux, Infosec and Tooling

Ishwor Gurung

- Software/Systems/Security engineer
- Python, Linux/BSDs
- Contact:
  - `ishw0r@irc.freenode.net`
  - `isg@email.badbug.id.au`

Conceptual Foundations

- Networking Concepts
- Linux kernel
- Public, Secret Key Cryptography (crypto is not trivial yo!)
- Web Application Issues
- Software Issues
- Tooling available

Networking Concepts

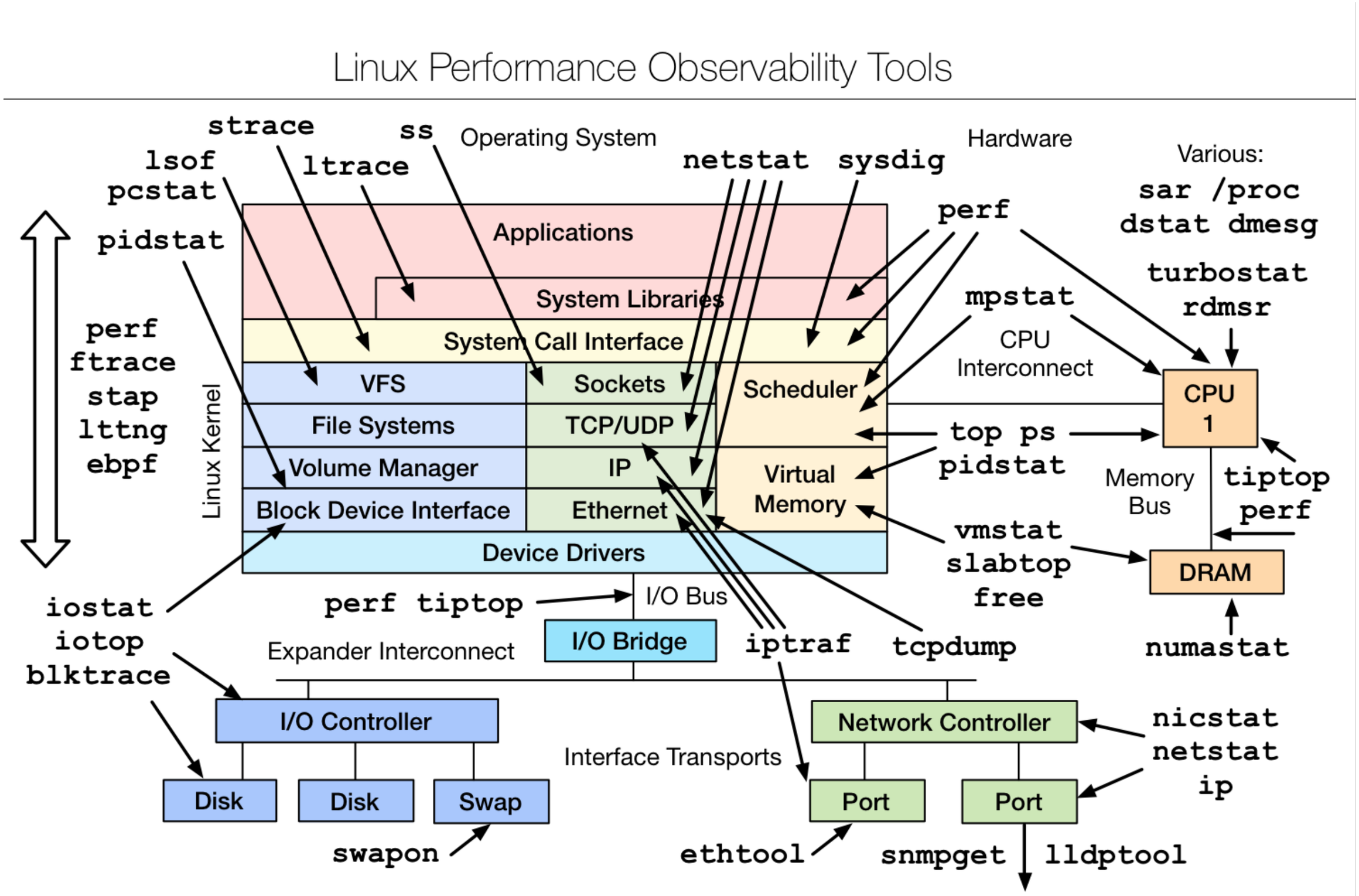
- OSI has seven layers, layer one important but usually left out of scope (Ethernet / USB)
- Layer two and beyond
  - MAC > IPv4 > TCP > TLS > HTML > Youtube
  - IPv4 (2^32) and IPv6 (2^128) publicly addressable endpoint addresses. IPv4 exhausted (NAT helps in this regard)
- Private subnet is 10.0.0.0/8, 192.168.0.0/16 and 172.16.0.0/12. Public subnet are the rest :)
- DNS(sec), HTTP, TLS, SMTP, VLAN, Routing, Switching, BGP(sec)

Linux

Linux (kernel)

- Process management - COW, `vfork`, `fork`, `task_struct`
- Process scheduling - process/thread state, pre-emptive scheduling, process CPU affinity, process address space, `mmap`
- System calls - interrupt and syscall handlers, `int` and `sysenter` interface
- Kernel drivers - top/bottom halves, interrupt driven, tasklets, work queues
- Kernel synchronisation - spinlocks (normal locks), mutexes and semaphores
- Memory management - **`kmalloc`**, **`vmalloc`**, slab allocation
- VFS - Inode, Dentry, Superblock
- Block I/O - Blockdev, I/O Schedulers

Linux (kernel)



http://www.brendangregg.com/linuxperf.html 2015

Web Application Issues

- OWASP Top 10
- Use freely available vulnerable web application VM images out on the internet
- Usual suspects
  - SQL injection
  - Cross-Site Scripting
  - Cross-Site Request Forgery
  - HTTP Request splitting
  - Command Injection
  - Remote File Inclusion
- Recommend Web Application Hacker's Handbook

Native Software Issues

- Buffer/Stack/Integer Overflows
- Memory Corruption
- Return-Oriented Programming (ROP chaining and gadgets)
- Smashing Stacks, Stack Canaries
- User Data Sanitisation (do not trust user input)
- Input/Output Boundary Validation (i repeat do not trust user input)
- Issues with “on-the-wire” protocol (padding/validation/parser)
- Support from the compiler vendors (SSP, FORTIFY_SOURCE, Propolice, Stackguard) and OS vendors on mitigating vulnerabilities
- OS level sandboxing (Linux, OSX, Windows)

Tools

- Remote access
  - `ssh`, `netcat`, `scp`, `rsync`
- Network troubleshoot
  - `tcpdump`, `ping/hping3`, `traceroute`, `netcat`, `mtr`, `wireshark`
  - `python`, `whois`, `nmap`, `dig` / `drill`, `lsof`, `netstat`
- WebApp Pentest
  - Burpsuite, Hackbar, Tamperdata, `curl`, code audit
- Distributed Workflow
  - `git`, Phabricator, JIRA, Confluence, Hipchat
- Infrastructure Pentest & Security
  - `iptables`, Linux hardening (principal of least authority), Acunetix, OpenVAS, Metasploit, SELinux/AppArmor, Roll your own kernel, aircrack-ng

nmap

- Good network exploration tool
- Provides support for host discovery, OS fingerprinting, Report generation
- Supports ping, ARP, XMAS/Kamikaze, FIN scans
- Supports different types of output format (XML, Simple)
- Various other libraries have sprung in the last decade to help craft packets easily but nmap still good for quick scans
- Leverage NSE (powerful)

openssh

- Secure Shell (replaces RSH)
- Provides a secure (and vetted) way to connect to machines (backed up by PKI)
- Transport, User and Connection Layer
- Supports various authentication methods
  - Password Auth - Sent encrypted by the client to the server
  - Public Key Auth - Server has access to the public key, client has private key, client send a signature created with the private key; Server verifies the signature is valid.
  - keyboard-interactive & GSSAPI authentication
- Transport layer handles key exchanges + server auth + encryption + compression + integrity.
- Configurable via `ssh_config` and `sshd_config`.

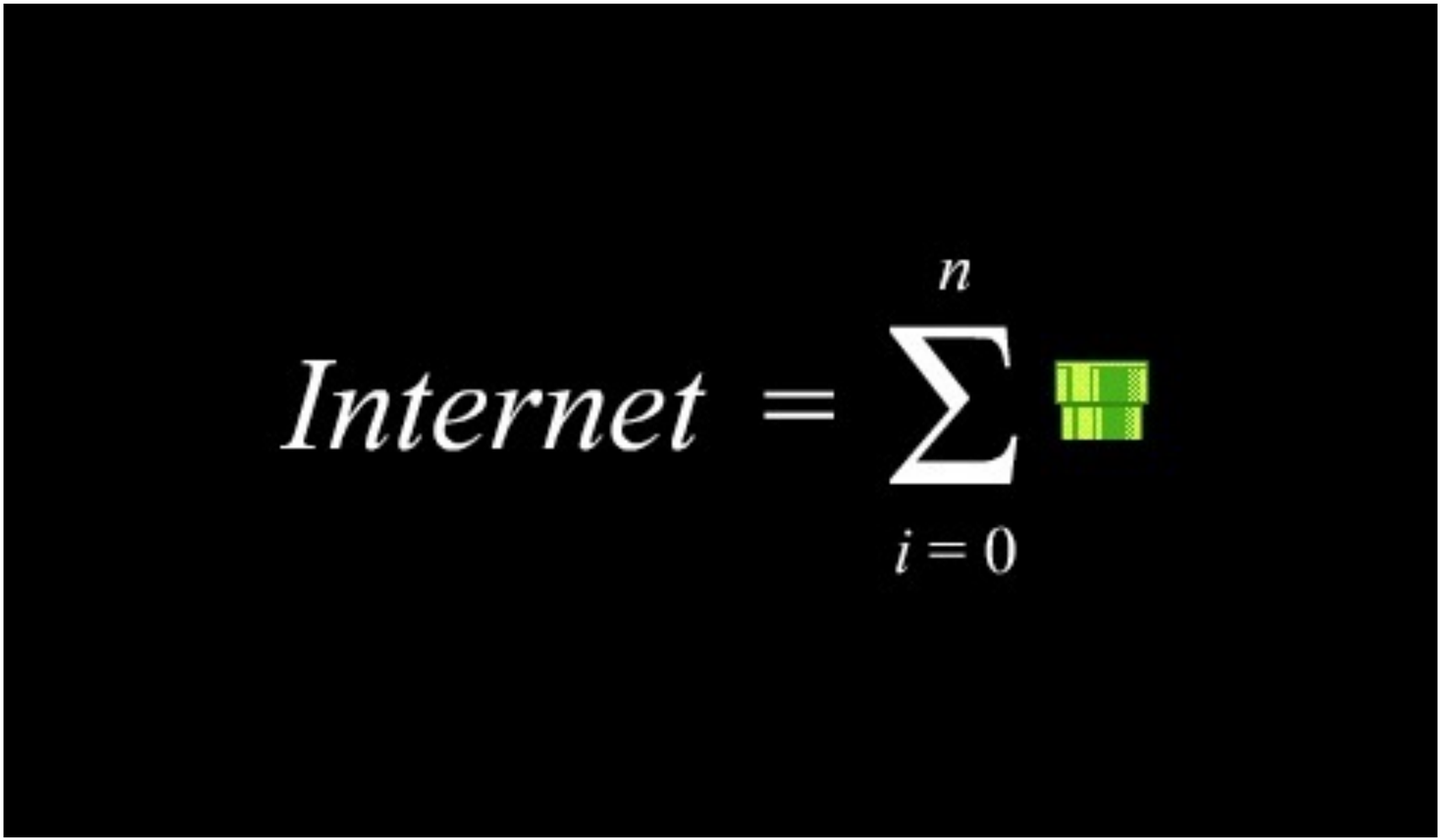
tcpdump

- Network traffic analyser
- Able to dump live packets on the wire and also able to read pcap files.
- Supports most L2-L7 network layers
- BPF filter expression
- Can glean into arbitrary packet characteristics (e.g. flags SYN, RST, URG etc.)
- Super handy tool to learn about networking and troubleshoot network.
- Not just “tcp/udp” packets: want to see what’s going on in the air: `tcpdump -c5 -i wlan0 -y IEEE802_11_RADIO`

application layer firewall

- Treating Network level spammers (like a boss) using `iptables`/`ipset` on Linux:
  - `/sbin/ipset create spams hash:ip family inet hashsize 32768 maxelem 327675`
  - `/sbin/ipset add spams 1.2.3.4`
  - `/sbin/iptables -A INPUT -p tcp -m multiport --dports 25,587,465,993 -j HAMMER`
  - `/sbin/iptables -A HAMMER -m set --match-set spams src -j REJECT --reject-with icmp-port-unreachable`
- Treating Network level spammers (like a boss) using `pf` on OpenBSD
  - `/etc/pf.conf` main config file
  - `drop` by default (`block drop`)
  - poke holes as needed (`pass in on $wan_if inet proto tcp to $wan_if port $emailports flags S/SA synproxy state rdr-to $emailservers`)
  - Want to drop bad bots?
    - `table <bots> persist file "/etc/zones/bots.zone"`
    - `block in quick on any from <bots> to any`

Series of tubes



traceroute

- Tracks the route packets taken from an IP network on their way to a given host.
- It utilises the IP protocol's time to live (TTL) field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to the host.
- `tcptraceroute` - tcp version

whois

- Looks up records in the databases maintained by several Network Information Centres, contacts whois registry

curl

- Powerful CLI tool to perform web requests
- Does almost 90% of what a browser can do with exception to JS

Burp Suite

- A great web application pentesting tool
- Supports wide array of HTTP verbs
- Provides MITM proxy via certificate pinning in the client
- Provides ability to perform automated tasks (e.g., session IDs enumeration) on the fly
- Provides repeater to manipulate HTTP/s query/body/header in a HTTP request

mitmproxy

- `pip install mitmproxy`
- `pip install httpie`
- `https_proxy=http://127.0.0.1:8080 http https://google.com`
- Great tool to have in the arsenal

Questions?

ishw0r@irc.freenode.net

isg@email.badbug.id.au